IoT Security Challenges and Issues: An Overview

[1]Prof. M.V.Shelke, [2]Prof. K.U.Jadhav, [3]Prof. P.D.Nanware
[123] Assistant Professor
[123]Computer Engineering Department,
[123]Sinhgad Academy of Engineering, Pune, India.

Abstract : Now a days physical environment are changed by the wireless sensor network. The wireless sensor network consists of number of tiny sensor nodes for sensing the environment with the limited computation and communication capabilities. The Internet of Things enabled by Wireless Sensor Networks (WSN) and RFID sensors finds a number of applications in almost all the fields such as health, education, transportation and agriculture. This paper briefs the idea of Internet of Things (IoT) and the security challenges to its future growth

IndexTerms **Wireless Sensor Network, (WSN), Internet of Things(IoT), RFID.**

I. INTRODUCTION

A Wireless Sensor Network has less or no infrastructure. It has number of sensor nodes and can work together to monitor a region to obtain data about the environment. The two types of WSNs called as structured WSN and unstructured WSN. Unstructured WSN contains dense collection of sensor nodes and often deployed in ad-hoc manner in field, i.e. nodes are deployed randomly in the target area. In structured WSN sensor nodes are deployed in pre-determined locations. These sensor nodes are used for specific application oriented. The characteristics of sensor networks are determined by using Data flow patterns and Energy constraints parameters.

The concept of IoT was firstly proposed by Kevin Ashton in 1999. The Internet of things is that it is the network in which every object or thing is provided unique identifier and data is transferred through a network without any verbal communication. Due to rapid growth in mobile communication, Wireless Sensor Networks (WSN), Radio Frequency Definition (RFID), and cloud computing, communications among IoT devices has become more convenient because IoT devices are capable of co-operating with one another. The fig. 1.1 shows the basic overview of internet of things.

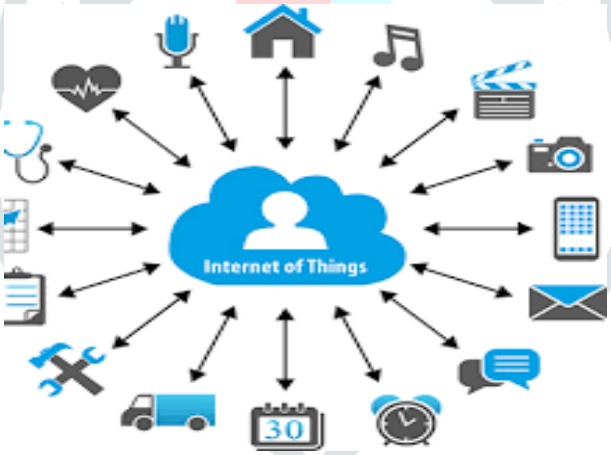

fig. 1.1: IoT

The major aim of IoT is in the formation of smart environments: smart homes, smart transport, smart items, smart cities, smart health, smart living, and etc.

II. CHARACTERISTICS OF IOT

- Dynamic Global network & Self-Adapting: The state of devices change dynamically, e.g., sleeping and waking up, connected and/or disconnected as well as the context of devices including location and speed. Moreover, the number of devices can change dynamically.
- Self Configuring: **:** IoT Devices have ability to configure themselves to provide certain functionality.
- Interoperable Communication Protocols: loT devices may support a number of interoperable communication protocols and can communicate with other devices and also with the infrastructure.
- Unique Identity: Each IoT device has a unique identity and a unique identifier (such as an IP address or a URI).
- Integrated into Information Network: IoT devices are integrated into the information network that allows them to communicate and exchange data with other devices and systems. IoT devices can be dynamically discovered in the network, by other devices and/or the network, and have the capability to describe themselves (and their characteristics) to other devices or user applications.

III. IoT Physical Design

The "Things" in IoT devices which have unique identity and can perform sensing, actuating and monitoring capabilities. IoT devices can exchange data or collect data from other connected devices and process data either locally or centralized server for further processing. Following block diagram shows typical structure of IoT device.

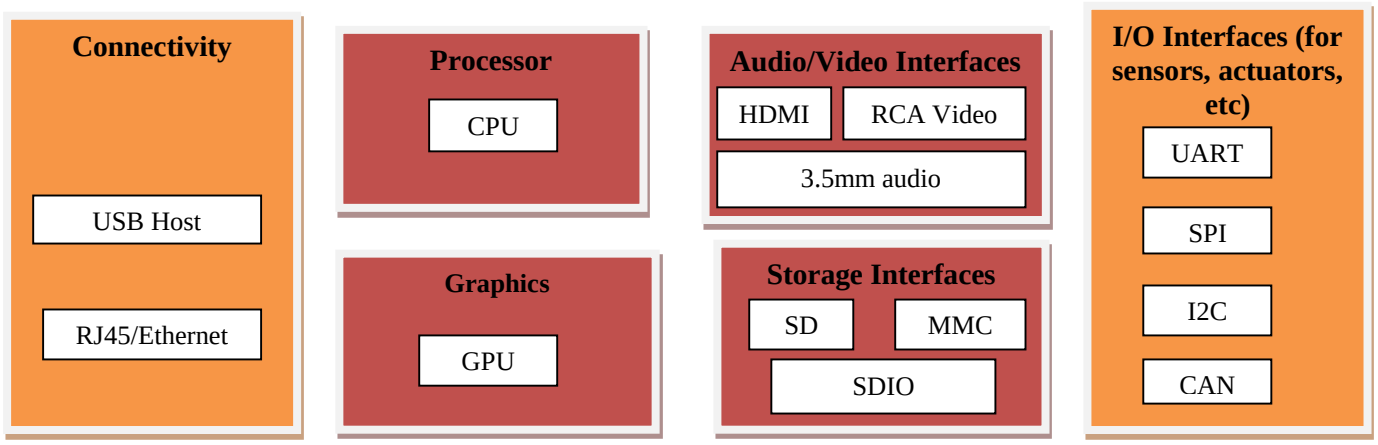

fig. 1.2: Generic block diagram of IoT

An IoT device may consist of several interfaces for connections to other devices, both wired and wireless. These include

i. I/O interfaces for sensors,
ii. interfaces for Internet connectivity,
iii. memory and storage interfaces and
iv. Audio/video interfaces.

IV. IOT APPLICATIONS

The scope of IoT is not limited to just connecting things to the internet but it allows communicating and exchanging data. The applications of IoT has wide range o domains such as homes, citites, environment, energy system, retail ,logistics agriculture an health few listed in fig. 1.3. For home, IoT has several applications such as smart lighting, smart appliances that can be remotely monitored and controlled. For cities ,IoT has applications such smart parking smart roads. Likewise each and every listed domains have specific IoT application.

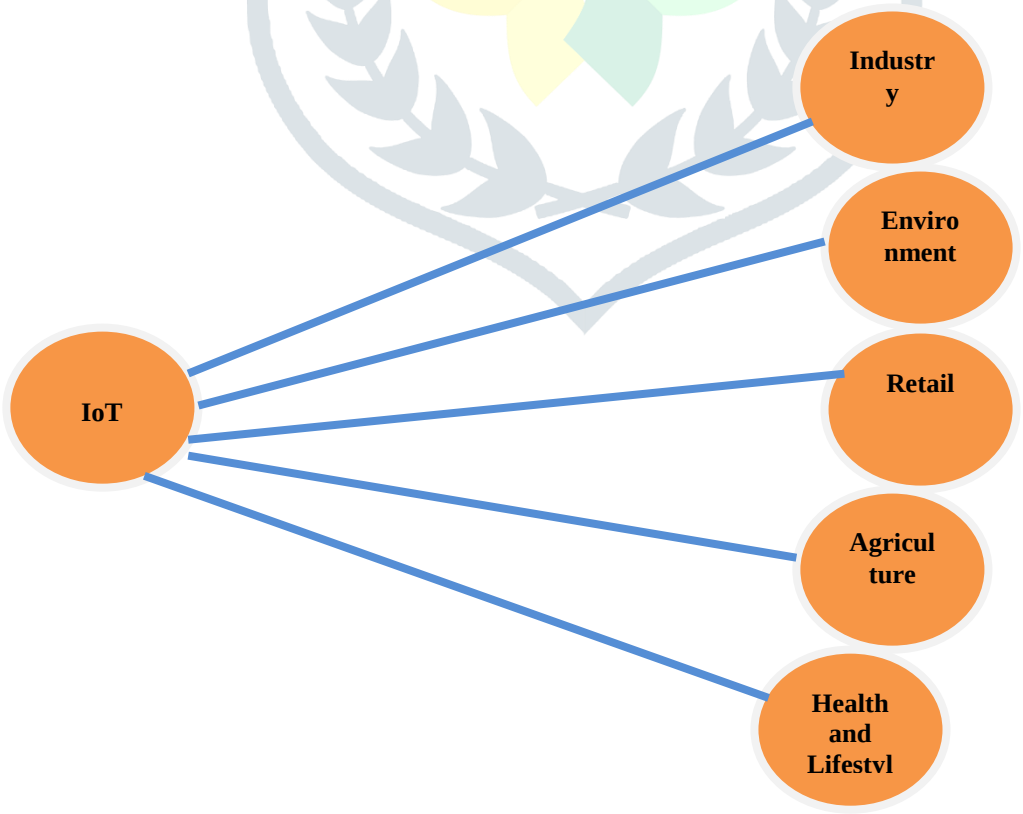

Fig.1.3: Applications of IoT

V. IoT SECURITY CHALLENGES AND ISSUES

In IoT, all the devices and people are connected with each other to provide services at any time and at anywhere. Most of the devices connected to the internet are not with efficient security mechanisms. So that they comes with various security issues e.g., confidentiality, integrity, and authenticity, etc. In other word IoT provides huge benefits, it is unable to provide various security threats in our daily life. The IoT consists of different devices and platform with different aspect, where every system needs the security requirement depending upon its application characteristics. As the number of connected IoT devices
Continually increase, security issues are exponentially multiplied and there are many security concerns need to be considered as an entire system. Privacy is one of the most important security issue because lots of user's personal information shared among various IoT devices. For example

1. Monitoring and personal information leakage: Safety is one of the important purposes of a smart home. Here there are a lot of sensors that are used for fire monitoring, baby monitoring, and housebreaking, etc. If these sensors are hacked by an intruder then he can monitor the home and access personal information. To avoid from this attack, data encryption must be applied between gateway and sensors or user authentication for the detection of unauthorized parties may be applied.
2. DoS/DDoS: Attackers may access the smart home network and send bulk messages to smart devices such as Clear To Send (CTS) / Request To Send (RTS). They can also attack targeted device by using malicious codes in order to perform DoS attacks on other devices that are connected in a smart home. Smart devices are unable to perform proper functionalities because of draining resources due to such attacks. For avoidance from this attack, it is very important to apply authentication to block and detect unauthorized access.
   As day by day Iot grows rapidly and security becomes important issue.

VI. IoT CHALLENGES

Sensors and Networking are the integral components of IoT. But not every machine is equipped with advanced sensors and networking capabilities to effectively communicate and share data. Following are few most significant challenges and problems that IoT is currently facing.

1. Scale: The scale of IT network is very large , the scale of OT can be several orders of magnitude larger.
2. Security: This is complex issue of IoT. AS more "things " get connected with other " things" and people security is increasing. If your device is get hacked then connectivity is major concern.
3. Privacy: As sensors become more creative in our everyday lives. They gather data will be specific to person and their activities. This data can range from health information to transactions information.
4. Big data and data analytics: With the help of sensors IoT collects huge amount of data. It is difficult to handle such data big data concept is used.

VII. SOME OTHER CHALLENGES

In above section we discussed about few important challenges faced by IoT except theses following challenges are faced by IoT.

- Meeting customer expectations
- Easing security concerns
- Keeping IoT hardware updated
- Overcoming connectivity issues
- Waiting for governmental regulation

VIII. CONCLUSION

The main emphasis of this paper was to brief idea about IoT and highlight major security issues of IoT and security attacks. Due to lack of security mechanism in IoT devices, many IoT devices become soft targets and even this is not in the victim's knowledge of being infected. In this paper, the security requirements are discussed such as confidentiality, integrity, and authentication, etc.

REFERENCES

[1] Mirza Abdur Razzaq, Muhammad Ali Qureshi, Sajid Habib Gill, Saleem Ullah,Security 2017 Issues in the Internet of Things (IoT): A Comprehensive Study, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 6
[2] Dr. B. Ramani , Dr. Anand Paul , 2016. INTERNET OF THINGS World Scient i f ic News 41 (2016) 1-304
[3] J. S. Kumar and D. R. Patel, , 2014. A survey on internet of things: Security and privacy issues, International Journal of Computer Applications, vol. 90, no. 11
[4] R. H. Weber, 2010. Internet of things–new security and privacy challenges, Computer law & security review, vol. 26, no. 1, pp. 23–30.
[5] A. Mohan, 2014 . Cyber security for personal medical devices internet of things, in Distributed Computing in Sensor Systems (DCOSS), IEEE International Conference on. IEEE, 2014, pp. 372–374.